На правах рукописи

Кочкарёв Александр Игоревич

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МНОГОБИТОВЫХ СИСТЕМ ЦИФРОВЫХ «ВОДЯНЫХ» ЗНАКОВ В УСЛОВИЯХ ВОЗМОЖНЫХ АТАК

05.12.13 – Системы, сети и устройства телекоммуникаций

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2019

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» на кафедре защищенных систем связи.

Научный руководитель: доктор технических наук, профессор,
Коржик Валерий Иванович

Официальные оппоненты:
Оков Игорь Николаевич,
доктор технических наук, профессор,
Филиал АО «Концерн радиостроения «Вега» в Санкт-Петербурге, ведущий научный сотрудник

Борисенко Николай Павлович,
кандидат технических наук, доцент,
ЗАО «Региональный Центр Защиты Информации «Форт», Центр системного анализа, начальник центра

Ведущая организация: Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский институт информатики и автоматизации Российской академии наук», Санкт-Петербург

Защита состоится 11 декабря 2019 года в 12.00 на заседании диссертационного совета Д 219.004.04, созданного при федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», по адресу: Санкт-Петербург, пр. Большевиков, д. 22, корп. 1, ауд. 554/1.

С диссертацией можно ознакомиться в библиотеке СПбГУТ по адресу Санкт-Петербург, пр. Большевиков, д. 22, корп. 1 и на сайте www.sut.ru.

Автореферат разослан 11 ноября 2019 года.

Ученый секретарь
диссертационного совета Д 219.004.04,
канд. техн. наук М.А. Маколкина

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. В настоящее время существует достаточно большой объем цифровых данных: фото, видео, документы, которые используются в нашей жизни, хозяйственной деятельности, требующих немедленной защиты от несанкционированного копирования и нелегального использования. Весьма актуальным является вопрос защиты авторских прав и интеллектуальной собственности, представленной в цифровом виде и передаваемой по каналам связи. Изображения, видеофайлы, будучи переданными по сети, могут претерпевать искажения, подвергаться сжатию и иной обработке. Раздел стеганографии – цифровые водяные знаки (далее – ЦВЗ), дают такую возможность по защите информации. Идея технологии ЦВЗ заключается в том, чтобы встроить невидимые «метки» внутрь защищаемого файла при условии сохранения его высокого качества, которые станут неотъемлемой его частью, устойчивые к попыткам удаления, и сохраняются на протяжении всего жизненного цикла файла. Реализацией данной идеи позволяет решить широкий ряд проблем защиты информации, передаваемой по сетям связи.

Система ЦВЗ – система, которая с помощью стеганографических методов обеспечивает безопасное хранение и передачу цифрового объекта (сигнал, неподвижное изображение, видео, звук) в сетях связи. Изображение при передаче по сети может быть подвергнуто сжатию (как с потерями, так и без), возможно добавление шумов – такие искажения (преобразования) изображения относятся к естественным. К ним ЦВЗ должен быть устойчив в первую очередь.

Особенно важно, чтобы цифровой водяной знак был устойчив к таким преобразованиям, как вырезание фрагмента. Достаточно просто осуществить вырезание части изображения и, если ЦВЗ после вырезания не сохранится, то совершенно бесполезна тогда будет его устойчивость к другим преобразованиям. К сожалению, большинство существующих разработанных цифровых водяных знаков не устойчиво к данному преобразованию, что ограничивает сферу их использования. Поэтому в данной работе делается упор на получение такой системы ЦВЗ, которая в первую очередь обеспечит «выживание» водяного знака после естественных преобразований изображения, которые происходят с ним в процессе его хранения, передачи по сетям связи и повседневного использования, прежде всего, непреднамеренно. Хотя также данные преобразования могут и выступать в качестве преднамеренных атак по удалению, к таким преобразованиям относятся: сжатие с потерями, вырезание фрагмента, добавление шума, нанесение сторонних изображений на исходное, вычеркивание строк и столбцов с их

последующей интерполяцией, масштабирование, поворот на угол, изменение яркости и контрастности.

Как правило, имеющиеся методы ЦВЗ невозможно надежно использовать без применения корректирующих кодов, подбор которых также является актуальным вопросом, по мнению большинства авторов современных ЦВЗ.

Поиск, разработка такого метода ЦВЗ, который обеспечит устойчивость к еще более обширному классу атак, чем уже имеющиеся методы могут обеспечить, является все еще актуальной задачей для того, чтобы имелась практическая возможность использовать цифровой водяной знак для наиболее сложного его предназначения – подтверждения прав собственности владельца защищаемого изображения и отслеживания нелегального распространения копий этого изображения в сети.

Степень разработанности темы. Работы по созданию систем цифровых водяных знаков ведутся отечественными и зарубежными учеными, начиная с конца 1990-ых годов. Основоположниками в данной области науки можно назвать таких ученых, как M. Barni, D. Benham, I. Cox, J. Fridrich, N. Komatsu и др. Наиболее значимые работы, посвященные разработке многобитовых цифровых водяных знаков пренадлежат таким ученым как A.M. Bruckstein, J. Ruanaidh, C. Hsu и J. Wu, P. Dong, J. Fridrich. К отечественным ученым-исследователям и разработчикам ЦВЗ можно отнести Коржика В.И., Анфиногенова С.О., Ушмоткина А.С., Федянина И.А., Земцова А.Н., Баранову Д.А.

Несмотря на весьма достаточную разработанность данной темы, даже в зарубежной литературе остается целый ряд нераскрытых вопросов, связанных с практическим использованием существующих систем ЦВЗ для защиты авторских прав на цифровые изображения и видео. Большинство из уже разработанных ЦВЗ позволяют ЦВЗ быть устойчивым только к узкому набору атак, которые может совершить злоумышленник для удаления ЦВЗ. Вопрос разработки систем ЦВЗ устойчивых к применению к ним более широкого спектра атак и преобразований остается открытым.

Объект исследования – алгоритмы вложения и извлечения цифровых водяных знаков в неподвижные изображения.

Предмет исследования – устойчивость цифровых «водяных» знаков к широкому спектру атак и преобразований таких, как вырезание фрагмента, масштабирование, поворот, сжатие, добавление шума.

Цели и задачи исследования. Целью исследования является повышение эффективности методов вложения и извлечения многобитовых ЦВЗ для защиты цифровых изображений, распространяемых в сети Интернет и передаваемых по

каналам связи, причем ЦВЗ должен быть устойчивым к удалению и должен сохранять высокое качество защищаемого изображения.

Для достижения сформулированной выше цели в диссертации поставлены и решены следующие научные задачи:

1. Исследование и тестирование известной ранее «голографической» системы ЦВЗ с целью выявления ее преимуществ и недостатков.

2. Оптимизация параметров «голографической» системы ЦВЗ для достижения одновременной устойчивости к таким видам преобразований изображения, как вырезание части изображения, добавление шума и сжатие JPEG, удаление строк и столбцов, поворот, масштабирование изображения, проведение теоретического обоснования стойкости предлагаемого метода к перечисленным искажениям.

3. Исследование возможности применения корректирующих кодов для повышения надежности вложения информации.

4. Исследование стойкости модифицированного «голографического» метода ЦВЗ к различным видам преобразований.

5. Поиск способов развития системы ЦВЗ для расширения устойчивости к еще более широкому спектру атак и преобразований.

Научная новизна результатов исследования. Данная работа обладает следующей новизной:

1. Впервые установлены данные по степени устойчивости бит вложенных в «голографический» ЦВЗ в зависимости от их расположения на частотной маске, и впервые к «голографическому» методу было переменено весовое декодирование и выявлены «надежные» биты;

2. Предложенный алгоритм извлечения «голографического» ЦВЗ из фрагментов стеганограммы является оригинальным алгоритмом, который учитывает доступную информацию (которая появляется в ходе решения проблемы регистрации) о совершенной атаке вырезания в отличие от первоначального алгоритма извлечения для «голографического» метода;

3. Впервые предложен реализуемый метод каскадирования ЦВЗ, объединяющий «голографический» и «нормализационный» методы ЦВЗ.

Теоретическая и практическая значимость работы. Теоретическая значимость в данной работе представляют: полученные данные для вероятностей ошибочного извлечения каждого вложенного бита в зависимости от примененной атаки. Установлено, что эти данные можно использовать в качестве весов при декодировании. Расширен класс методов извлечения «голографического» ЦВЗ. В рамках данной работы решен ряд теоретических вопросов построения каскадной

системы ЦВЗ, таких как порядок вложения бит информации, определение наиболее доверительной цепочки бит после извлечения.

Практическая значимость полученных результатов заключается в том, что разработанную в результате работы многобитовую систему ЦВЗ, которая включает в себя «голографическую» систему ЦВЗ, оптимизированную с точки зрения использования бит маски, дополненную весовым декодированием, корректирующими кодами, оптимальным алгоритмом извлечения ЦВЗ из фрагментов стеганограммы, а также каскадную систему ЦВЗ можно с высокой степенью надежности использовать для защиты цифровых неподвижных растровых изображений, в том числе, и для сценария отслеживания «отпечатков пальцев».

Полученный модифицированный «голографический» метод ЦВЗ с использованием весового декодирования обладает устойчивостью к атакам сжатия JPEG, добавлению шума на порядок выше, чем может обеспечить изначальный «голографический» метод.

Предложенный алгоритм извлечения «голографического» ЦВЗ из фрагментов стеганограммы позволяют «голографическому» ЦВЗ быть наиболее устойчивым к атаке вырезания, либо позволяют расширить количество вкладываемых бит.

Каскад ЦВЗ, объединяющий «голографический» и «нормализационный» методы ЦВЗ, обладает большей устойчивостью к атакам, чем применение его слагаемых ЦВЗ по отдельности. В итоге «каскадный» метод ЦВЗ обеспечивается устойчивость к таким преобразованиям и атакам, как: вырезание фрагментов изображения; сжатие JPEG; добавление шума; нанесение графических элементов поверх исходного изображения; изменение контрастности; удаление строк и столбцов с последующей интерполяцией; масштабирование; поворот. Представленные эксперименты по изучению устойчивости ЦВЗ к различным атакам и преобразованиям могут быть полезны для воспроизведения и тестирования других методов ЦВЗ.

Методология и методы исследования. Для решения поставленных задач использовались теоретические методы, основанные на разделах прикладной математики, таких как теория вероятности и математическая статистика, помехоустойчивое кодирование, а также методы компьютерного моделирования, тестирования и программирования на языке Matlab.

Положения, выносимые на защиту.

1. Модифицированный «голографический» метод ЦВЗ с использованием весового декодирования.

2. Оптимальный алгоритм извлечения «голографического» ЦВЗ из фрагментов стеганограммы.

3. Каскадная схема вложения ЦВЗ с использованием «голографического» и «нормализационного» методов вложения ЦВЗ.

Степень достоверности и апробация результатов. Достоверность полученных результатов подтверждается совпадением результатов теоретического обоснования и результатов экспериментов, полученных с помощью компьютерного моделирования.

Результаты данной диссертационной работы апробированы на международных научных конференциях, в том числе: "Federated Conference on Computer Science and Information Systems 2013" (г. Краков, 2013), «Интернет: информационные технологии и инженерные разработки» (Санкт-Петербург, 2011), Международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» № 64 (Санкт-Петербург, 2012, 2013).

Результаты исследований использованы АО «Научные приборы», ООО «Дигитон», ООО «Лид тайм», что подтверждается актами об использовании и внедрении результатов диссертационной работы.

Публикации. Основные результаты диссертационного исследования опубликованы в 10-ти научных трудах из них: 3 – в рецензируемых научных изданиях из Перечня ВАК; 2 – в научных изданиях, индексируемых в международных базах цитирования, 5 – в сборниках научных статей, трудов, тезисов докладов и материалах конференций.

Соответствие паспорту специальности. Представленные в данной работе исследования соответствуют пункту 10 специальности 05.12.13 – Системы, сети и устройства телекоммуникаций: *Исследование и разработка новых методов защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций*, поскольку исследованные и разработанные в данной диссертации системы цифровых водяных знаков обеспечивают безопасность прав собственности для цифровых данных, передаваемых в сетях связи.

Личное участие соискателя. Все основные результаты диссертации получены соискателем лично. Автор диссертации лично проводил исследование и предлагал новые алгоритмы для решения поставленных задач, проводил программное моделирование, осуществлял анализ полученных данных. Научным руководителем проводились обсуждение и контроль полученных результатов. Часть публикаций по проведенным исследованиям написана лично, а часть в соавторстве совместно с научным руководителем, д.т.н., профессором В.И. Коржиком.

Структура и объем диссертации. Диссертационная работа состоит из введения, основной части (содержащей 4 раздела), заключения, списка литературы и приложений. Общий объем работы – 142 страницы, из них основного текста – 135 страниц. Работа содержит 45 рисунков и 22 таблицы. Список литературы включает 53 библиографических источника.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** дано обоснование актуальности темы исследований, сформулированы цели и задачи исследований, приведены основные научные положения, выносимые на защиту, выделена научная новизна и практическая ценность полученных результатов, приведены сведения об апробации работы.

В **первой главе** даются основные определения, понятия, касающиеся цифровых водяных знаков, направления их использования, представлен обзор существующих методов ЦВЗ и направления развития в их разработке.

Во **второй главе** приведены результаты исследования «голографического» метода ЦВЗ, в том числе выявление его преимуществ и недостатков.

Голографический метод впервые был предложен А. Брукштейном1[1]. Вложение голографическим методом осуществляется по правилу:

$$I^{w}(x,y) = FT^{-1}\{W_M(u,v)\cdot FT\{I(x,y)\}\}, \quad (1)$$

где $I^{W}(x,y)$ – изображение с вложением ЦВЗ (стеганограмма);

$I(x,y)$ – исходное изображение;

$FT\{\ldots\}$ – прямое двумерное преобразование Фурье;

$FT^{-1}\{\ldots\}$ – обратное двумерное преобразование Фурье;

$W_M(u,v)$ – маска, $W_M(u,v) = 1 \pm \varepsilon(u,v)$.

При этом предлагается вкладывать каждый n-ый бит ЦВЗ посредством создания маски (рис. 1), состоящей из секторов R_n. Каждый такой сектор разбивается на две подобласти R_{n1}, R_{n2}, и вложениеn-го бита b_n выполняется по правилу:

$$\text{Если } b_n = 0, \quad \begin{cases} W(u,v) = 1 + \boldsymbol{\varepsilon} & (u,v) \in R_{n,1} \\ W(u,v) = 1 - \boldsymbol{\varepsilon} & (u,v) \in R_{n,2} \end{cases},$$

$$\text{Если } b_n = 1, \quad \begin{cases} W(u,v) = 1 - \varepsilon & (u,v) \in R_{n,1} \\ W(u,v) = 1 + \varepsilon & (u,v) \in R_{n,2} \end{cases}, \quad (2)$$

[1] Bruckstein, A.M. A holographic transform domain image watermarking method / A.M. Bruckstein, T.J. Richardson // Circuits, Systems and Signal Processing. – 1998. – Т. 17. – №. 3. – С. 361-389.

где $\varepsilon(u, v)$ – области маски с постоянной глубиной вложения ε.

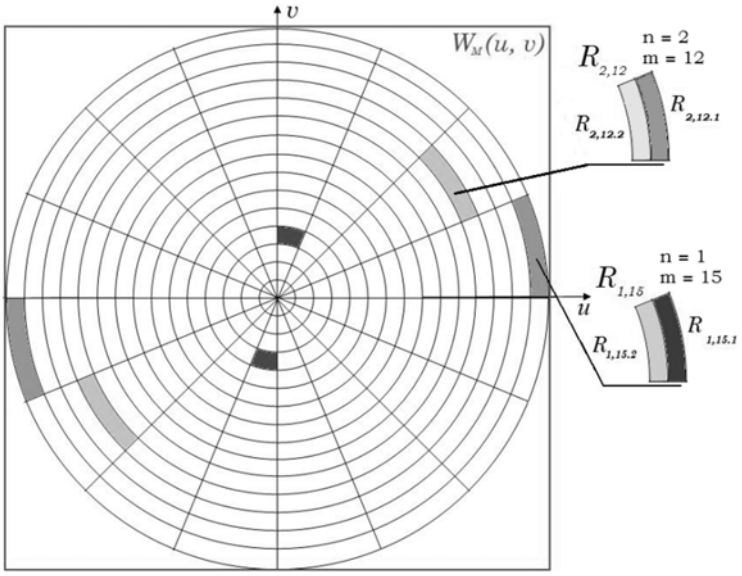

Рисунок 1 – Разбиение «равнорадиусной» частотной маски на сектора

Извлечение ЦВЗ производится по следующему правилу:

$$\frac{\sum_{i \in R_{n,1}} \mathrm{Re}(q_i^* \cdot s_i)}{\sum_{i \in R_{n,1}} |s_i|^2} \underset{b_n = 0}{\overset{b_n = 1}{<}} \frac{\sum_{i \in R_{n,2}} \mathrm{Re}(q_i^* \cdot s_i)}{\sum_{i \in R_{n,2}} |s_i|^2}, \tag{3}$$

где q_i – значение комплексных коэффициентов Фурье изображения с вложением ЦВЗ;

s_i – значение комплексных коэффициентов Фурье исходного изображения;

«*» – знак комплексного сопряжения.

Как видно из (3), для извлечения ЦВЗ требуется знание оригинального изображения и обеспечение совмещения его с исходным изображением (т.е. решение проблемы *регистрации*).

«Голографическим» данный метод называется, поскольку использует, так называемые, «голографические» преобразования. Они позволяют цифровому водяному знаку быть выделенным даже по малой части, «вырезанной» из стеганограммы. Такое свойство характерно для голограмм в оптике, когда любой фрагмент голограммы содержит в себе информацию о целом объекте, что и определило «метафорическое» название этих преобразований А. Брукштейном. В действительности же, для ЦВЗ «голографическое» свойство обеспечивается за счет использования преобразования Фурье, маски определенной структуры и разностного кодирования вкладываемых в неё бит.

В рамках диссертационной работы было проведено компьютерное моделирование «голографического» метода ЦВЗ, а затем проведены исследования по устойчивости данного метода при различных параметрах вложения, а также влияние вложения ЦВЗ на качество изображения. В исследовании была использована тысяча изображений из базы изображений, которая специально предназначена для тестирования стегосистем.

В табл. 1 представлены результаты исследования устойчивости ЦВЗ при вложении 120 бит информации при «равнорадиусной» геометрии маски (см. рис. 1), для параметров $N = 8$ (количество лучей в верхней полуплоскости маски), $M = 15$ (количество окружностей в маске), и глубине вложения $\varepsilon = 0{,}05$. Для получения данной статистики использовались 8 битные изображения с градациями серого размером 512×512 пикселей.

Таблица 1 – Результаты экспериментов по устойчивости оригинального голографического метода ЦВЗ

Преобразование	Процент ошибочно извлеченных бит, %
Вырезание фрагмента до **200 × 200 пикселей**	0
Вырезание фрагмента до**170 × 170 пикселей**	7
Форматирование JPEG с $Q = 60\%$	0
Форматирование JPEG с $Q = 50\%$	до 5
Форматирование JPEG с $Q = 20\%$	до 25
Форматирование JPEG с $Q = 10\%$	до 35
Добавление гауссовского шума с дисперсией $d = 25$	до 15
Поворот стеганограммы на угол 1º без компенсации	до 40

Из данных результатов видно, что ЦВЗ устойчив к вырезанию даже достаточно малых фрагментов изображения и JPEG-сжатию с потерями. Наблюдается значительное количество ошибок при сжатии с $Q < 30\%$, при применении гауссовского шума с дисперсией $d > 25$, однако качество изображения при данных преобразованиях можно считать неприемлемым для коммерческого использования.

Детальное изучение такой системы ЦВЗ показало, что биты извлекаются с неодинаковой вероятностью ошибки, поскольку они априорно «погружаются» в разные секторы маски, которые в свою очередь оказывают различное воздействие на разные частотные составляющие амплитудного спектра. Зависимости вероятностей извлечения бит из конкретного сектора маски после различных преобразований изображения с вложением в диссертации сведены в

соответствующие таблицы (в качестве примера представлены таблицы 2-3). Одним из выявленных недостатков метода является необходимость решать проблему «регистрации» и зависимость эффективности метода от успешности ее решения. Так, если извлечение происходит из стеганограммы, подвергнутой повороту и угол поворота был недостаточно скомпенсирован в ходе решения проблемы регистрации, то количество ошибок при извлечении будет недопустимо большим.

Таблица 2 – Вероятности ошибочного извлечения бит (в процентах) в зависимости от области маски (*n, m*) после извлечения ЦВЗ из фрагмента 200×200 пикселей

*n**m*	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	43	9	2	0	1	0	0	1	0	0	0	0	1	1	3
2	38	1	2	0	0	0	0	0	0	0	0	0	0	1	0
3	43	13	0	1	1	0	1	0	1	0	0	0	1	0	0
4	32	3	1	1	0	1	2	3	2	2	5	5	6	3	5
5	46	2	1	1	1	1	1	1	1	1	2	2	3	2	3
6	25	3	1	1	1	0	1	0	0	2	0	2	2	1	0
7	23	2	1	1	1	0	1	0	0	0	0	1	0	0	0
8	45	3	1	1	0	0	1	0	0	0	1	0	0	0	2

Таблица 3 – Вероятности ошибочного извлечения бит (в процентах) в зависимости от области маски (*n, m*) после сжатия JPEG с качеством $Q = 10\%$

*n**m*	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	3	1	4	3	7	21	39	34	32	42	48	38	52	46	47
2	3	2	5	16	19	31	44	35	49	47	49	41	56	44	38
3	2	0	4	12	19	36	29	45	42	42	45	56	50	46	44
4	3	0	1	8	6	15	25	40	43	50	55	48	38	47	46
5	2	2	2	5	10	15	32	35	41	48	51	43	48	48	39
6	2	3	4	7	21	28	43	53	44	45	50	44	57	51	45
7	0	1	4	15	27	36	46	36	45	42	53	44	50	45	53
8	0	1	1	5	8	28	35	40	41	40	38	47	44	51	50

В **третьей главе,** на основе полученных результатов экспериментов предыдущего раздела, предложено усовершенствование «голографического» метода ЦВЗ. Первым способом усовершенствования является выделение «надежных» бит из общего их числа. Из таблиц 2-3 видно, что такие преобразования, как добавление гауссовского шума, сжатие JPEG приводят к возрастанию вероятности ошибочного извлечения для бит, погруженных в

высокочастотные области маски ($m \geq 8$) (m – номер луча в маске или координата области $\boldsymbol{R_{n,m}}$). Атака по вырезанию фрагмента приводит к возрастанию вероятности ошибочного извлечения (см. таблицы 2-3), в том числе, и для бит, погруженных в низкочастотные области маски ($m \leq 2$). Таким образом, из исходных 120 вложенных бит можно выделить лишь около 64 бит, которые извлекаются с допустимой вероятностью ошибки при различных видах преобразований и атак (эти биты выделены серым цветом в таблицах 2-3). Будем далее называть данные биты ($9 \geq m \geq 2$) *«надежными»* битами.

Таблица 4 – Вероятности ошибочного декодирования при использовании различных БЧХ-кодов при различных атаках и декодировании по минимальному расстоянию Хемминга и по весовому декодированию

БЧХ-коды	(63, 7)	(63, 10)	(63, 16)	(63, 7)	(63, 10)	(63, 16)
Способ декодирования	по минимальному расстоянию Хемминга			по весовому декодированию		
Сжатие JPEG с $Q = 20\%$	$2{,}3 \cdot 10^{-2}$	$4{,}7 \cdot 10^{-2}$	$7{,}9 \cdot 10^{-2}$	$1{,}5 \cdot 10^{-3}$	$4{,}1 \cdot 10^{-3}$	$1{,}0 \cdot 10^{-2}$
Сжатие JPEG с $Q = 30\%$	$5{,}7 \cdot 10^{-3}$	$1{,}4 \cdot 10^{-2}$	$2{,}5 \cdot 10^{-2}$	$1{,}0 \cdot 10^{-4}$	$1{,}0 \cdot 10^{-3}$	$3{,}5 \cdot 10^{-3}$
Сжатие JPEG с $Q = 60\%$	$1{,}2 \cdot 10^{-3}$	$1{,}7 \cdot 10^{-3}$	$3{,}8 \cdot 10^{-3}$	$1{,}0 \cdot 10^{-4}$	$1{,}0 \cdot 10^{-4}$	$1{,}0 \cdot 10^{-4}$
Вырезание фрагмента 200×200 пикселей	$1{,}5 \cdot 10^{-2}$	$2{,}0 \cdot 10^{-2}$	$2{,}8 \cdot 10^{-2}$	$4{,}3 \cdot 10^{-3}$	$9{,}1 \cdot 10^{-3}$	$1{,}6 \cdot 10^{-2}$
Вырезание фрагмента 250×250 пикселей	$4{,}1 \cdot 10^{-3}$	$5{,}5 \cdot 10^{-3}$	$7{,}9 \cdot 10^{-3}$	$2{,}1 \cdot 10^{-3}$	$3{,}0 \cdot 10^{-3}$	$4{,}7 \cdot 10^{-3}$
Удаление 20 строк и 20 столбцов	$5{,}0 \cdot 10^{-3}$	$1{,}2 \cdot 10^{-2}$	$2{,}5 \cdot 10^{-2}$	$4{,}0 \cdot 10^{-4}$	$1{,}3 \cdot 10^{-3}$	$3{,}9 \cdot 10^{-3}$
Добавление гауссовского шума с дисперсией $d = 25$	$1{,}3 \cdot 10^{-2}$	$2{,}3 \cdot 10^{-2}$	$3{,}9 \cdot 10^{-2}$	$2{,}0 \cdot 10^{-3}$	$4{,}3 \cdot 10^{-3}$	$1{,}2 \cdot 10^{-2}$

В первоначальном «голографическом» методе ЦВЗ оставался также открытым вопрос об использовании корректирующих кодов (а именно БЧХ кодов), который был решен в рамках данной главы диссертации (см. табл. 4).

Предложен алгоритм весового декодирования (4), где в качестве весов используются предварительно построенные таблицы вероятностей ошибочного извлечения каждого бита при определенной атаке и преобразовании (табл. 2-3)

$$\tilde{j} = \arg\max_{j} \left[\prod_{i \in I(e_{j1})} P_i \cdot \prod_{i \in I(e_{j0})} (1 - P_i) \right], \qquad (4)$$

где $\tilde{j}$ – номер кодовой группы после декодирования,

P_i – вероятность битовой ошибки в i-м бите,

$I(e_{j1})$ – набор единиц из вектора e_j,

$I(e_{j0})$ – набор нулей из вектора e_j,

$$e_j = u \oplus v_j,$$

где u – принятый 63-битный вектор после декодирования,

v_j – j кодовое слово БЧХ-кода.

Такой метод декодирования позволяет учесть особенности каждого из преобразований (сжатия JPEG, вырезание фрагмента, и других), т.к. каждый из них влияет на свою часть спектра, и, следовательно, в одном случае при декодировании некоторым битам можно доверять больше чем другим; тем самым, оказывается возможным уменьшить вероятность ошибки при извлечении информационных бит. Сравнение декодирования по минимальному расстоянию Хемминга и весового декодирования представлено в таблице 4. Применение весового декодирования дает уменьшение вероятности ошибочного декодирования кодовых слов.

Сильная сторона голографического метода заключается в том, что он позволяет ЦВЗ быть устойчивым, прежде всего, к атаке вырезанием фрагмента стеганограммы. Однако именно вопрос техники извлечения ЦВЗ из фрагмента стеганограммы оставался не проработанным до конца. В данной диссертационной работе предложен новый алгоритм извлечения ЦВЗ из фрагмента стеганограммы оптимальным «голографическим» декодером. Первоначальное решающее правило (3) не учитывало параметры совершенной атаки, в том числе и атаки вырезания. Поскольку у голографической системы ЦВЗ декодер информированный (для извлечения используется оригинальное изображение), то имеется возможность предсказать величины коэффициентов Фурье стеганограммы, подверженной атаке вырезанием, и учесть полученные величины в решающей схеме при извлечении ЦВЗ.

Представим вложение информации в пару подобластей (R_{n1},R_{n2}) в виде правила:

$$\tilde{s}_i = \begin{cases} s_i(1+\varepsilon), i \in R_{n1} \\ s_i(1-\varepsilon), i \in R_{n2} \end{cases} \text{ при вложении } b_n = 0 \text{ в область } (R_{n1},R_{n2}),$$

$$\tilde{s}_i = \begin{cases} s_i(1-\varepsilon), i \in R_{n1} \\ s_i(1+\varepsilon), i \in R_{n2} \end{cases} \text{ при вложении } b_n = 1 \text{ в область } (R_{n1},R_{n2}),$$

где s_i – значение коэффициентов Фурье исходного изображения;

$\tilde{s}_i$ – значение коэффициентов Фурье изображения с вложением.

Обозначим $\tilde{s}_{i0} = s_i(1+\varepsilon)$, $\tilde{s}_{i1} = s_i(1-\varepsilon)$.

Поскольку выполняется атака вырезания фрагмента, то после такого преобразования получаем:

$$s_{i0} = Cr(s_i(1+\varepsilon)),\ s_{i1} = Cr(s_i(1-\varepsilon)),$$

где *Cr*() – преобразование «вырезание фрагмента», примененное ко всему изображению в пиксельной области.

Обозначим также вектором $\boldsymbol{Q} = (q_1, q_2, \dots, q_N)$ комплексные коэффициенты Фурье в области (R_{n1}, R_{n2}) после вложения, применения атаки вырезания фрагмента и добавления аддитивного шума.

Предположим, что реализация шумовых помех распределена по гауссовскому закону с параметрами (0, σ^2). Тогда многомерное распределение коэффициентов $\boldsymbol{Q}$ при вложении в область (R_{n1},R_{n2}) «0» или «1» соответственно будет иметь вид:

$$W(\boldsymbol{Q}|b_n = 0) = \prod_{i\in R_{n1}} \frac{1}{2\pi\sigma^2} \cdot e^{-\frac{1}{2\sigma^2}\cdot|q_i - s_{i0}|^2} \prod_{i\in R_{n2}} \frac{1}{2\pi\sigma^2} \cdot e^{-\frac{1}{2\sigma^2}\cdot|q_i - s_{i1}|^2},$$

$$W(\boldsymbol{Q}|b_n = 1) = \prod_{i\in R_{n1}} \frac{1}{2\pi\sigma^2} \cdot e^{-\frac{1}{2\sigma^2}\cdot|q_i - s_{i1}|^2} \prod_{i\in R_{n2}} \frac{1}{2\pi\sigma^2} \cdot e^{-\frac{1}{2\sigma^2}\cdot|q_i - s_{i0}|^2},$$

где |…| – модуль комплексного числа.

Вычислим теперь логарифм отношения правдоподобия:

$$\lambda(\boldsymbol{Q}) = \log\left(\frac{W(\boldsymbol{Q}|b_n = 1)}{W(\boldsymbol{Q}|b_n = 0)}\right) =$$

$$= \sum_{i\in R_{n1}} \frac{1}{2\sigma^2}(-|q_i - s_{i1}|^2 + |q_i - s_{i0}|^2) + \sum_{i\in R_{n2}} \frac{1}{2\sigma^2}(-|q_i - s_{i0}|^2 + |q_i - s_{i1}|^2).$$

Далее можно убрать постоянный множитель $\frac{1}{2\sigma^2}$, что дает:

$$\tilde{\lambda}(\boldsymbol{Q}) = \sum_{i\in R_{n1}}(-|q_i - s_{i1}|^2 + |q_i - s_{i0}|^2) + \sum_{i\in R_{n2}}(-|q_i - s_{i0}|^2 + |q_i - s_{i1}|^2). \quad (4)$$

Решающее правило принимает после этого следующий вид:

$$b_n\text{=1, если } \tilde{\lambda}(\boldsymbol{Q}) \geq 0; \quad (5)$$

$$b_n\text{=0, если } \tilde{\lambda}(\boldsymbol{Q}) < 0.$$

Подставляя (4) в (5), окончательно получаем:

$$\sum_{i\in R_{n1}}|q_i - s_{i1}|^2 - |q_i - s_{i0}|^2 \underset{b_n = 0}{\overset{b_n = 1}{\lessgtr}} \sum_{i\in R_{n2}}|q_i - s_{i1}|^2 - |q_i - s_{i0}|^2. \quad (6)$$

Решающее правило (6) отличается от аналогичного правила (3) тем, что учитывает атаку вырезания в полной мере. И также является оптимальным по критерию максимального правдоподобия, получено в предположении, что реализация шумовых помех распределена по гауссовскому закону. Как показали результаты моделирования, оптимальный метод извлечения дает достаточно малые вероятности ошибки извлечения бит, что позволяет расширить диапозон

«надежных» бит. Экспериментально полученные вероятности ошибочного извлечения бит при применении правила (6) и вырезании фрагмента 200×200 пикселей представлены в таблице 5 (полезно сравнить её с данными таблицы 2). В диссертационной работе представлены также и подоптимальные методы, которые уступают оптимальному методу в помехоустойчивости, но, если требуется, могут понизить вычислительную сложность вычислений при извлечении ЦВЗ.

Таблица 5 – Вероятности ошибочного извлечения бит при оптимальном методе и вырезании фрагмента 200×200 пикселей при ε = 0,1 и равнорадиусной геометрии маски (значения вероятностей указаны в %)

*n**m*	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	3	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2	3	1	0	0	0	0	0	0	0	0	0	0	0	0	0
3	2	0,5	0	0	0	0	0	0	0	0	0	0	0	0	0
4	1	1	0,5	0	0	0	0	0	0	0	0	0	0	0	0
5	1	0,5	0,5	0	0	0	0	0	0	0	0	0	0	0	0
6	1	0,5	0	0	0	0	0	0	0	0	0	0	0	0	0
7	1	0,5	0,5	0	0	0	0	0	0	0	0	0	0	0	0
8	1,5	0,5	0	0	0	0	0	0	0	0	0	0	0	0	0

Также в данной главе решается вопрос увеличения скорости вложения для «голографических» систем ЦВЗ. Для решения этой проблемы предлагается, во-первых, использовать оптимальный метод при извлечении из фрагментов ЦВЗ, что дает нам увеличение количества «надежных» бит в области низких частот. Во-вторых, предлагается использовать для вложения большего размера (1024×1024 и более). В-третьих, предлагается использовать в качестве критерия для построения маски – количество коэффициентов Фурье (пикселей) в самой малой из областей для вложения. Так, при гарантированной устойчивости ЦВЗ к атакам вырезания до четверти изображения, сжатия JPEG, добавления гауссовского шума с $d = 20$ в изображение размером 1024×1024 возможно вложить порядка 100-150 бит. Варьирование скорости обуславливается влиянием статистики исходного изображения на устойчивость ЦВЗ к атакам.

В **четвертой** главе описан предложенный каскадный метод ЦВЗ. «Голографический» метод со всеми предложенными модификациями требует решения проблемы регистрации. От успешности решения проблемы регистрации зависит конечный результат надежности извлечения бит ЦВЗ (так нескомпенсированный в процессе решения проблемы регистрации поворот на угол

в 1º или масштабирование в 101% может привести к появлению ошибок). Данную проблему можно устранить путем усовершенствования применяемых методов регистрации, но существует и принципиально иной путь решения – организовать систему с повторным вложением, когда вложение бит осуществляется не только голографическим методом ЦВЗ, но и дополнительным методом ЦВЗ, который устойчив к преобразованиям поворота и масштабирования. В качестве такого дополнительного метода ЦВЗ можно использовать, так называемый, «нормализационный» метод[2].

«Нормализационный» метод ЦВЗ позволяет обеспечить извлечение ЦВЗ из стеганограммы, которая подверглась ранее геометрическим преобразованиям, в частности масштабированию и повороту. Основная идея метода заключается в том, чтобы получить нормализованное изображение, которое всегда будет одним и тем же, как для исходного оригинального изображения, так и для оригинального изображения, подвергнутого различным афинным геометрическим преобразованиям. Данный метод ЦВЗ был промоделирован и исследован на предмет устойчивости к атакам вырезания фрагментов, сжатию JPEG, добавлению гауссовского шума, повороту, масштабированию.

Два подхода в организации каскада, состоящего из голографического и нормализационного методов, представлены на рис. 2. Качество изображения после каскадного вложения остаётся приемлемым; влияние методов друг на друга присутствует, но может быть сведено к минимуму при правильном порядке вложения методов.

а)

б)

Рисунок 2 – Подходы в организации каскада ЦВЗ: (а) Г→Н, (б) Н→Г

[2] Dong, P. Digital watermarking robust to geometric distortions / P. Dong, J.G. Brankov, N.P. Galatsanos, Y. Yang, F. Davoine // IEEE Transactions on Image Processing. – 2005. – V. 14. – No. 12. – P. 2140-2150.

Было доказано при помощи моделирования, что более предпочтительным оказывается каскадное вложение по схеме Г→Н (рис. 2(а)), где вложение осуществляется сначала голографическим методом, а затем нормализационным.

Предложено использовать корректирующие коды БЧХ для корректирования ошибок и выбора наиболее доверенной цепочки бит после извлечения. Достаточно для этого подсчитать расстояние Хемминга между полученной цепочкой бит и ближайшим разрешенным кодовым словом и сравнивать его с выбранным порогом λ.

$$\begin{cases} \min d_i < \min d_j \\ \min d_i < \lambda, \end{cases}, \tag{7}$$

где d_i – расстояние Хемминга i-го кодового слова для первого метода ЦВЗ в каскаде,

d_j – расстояние Хемминга j-го кодового слова для второго метода ЦВЗ в каскаде,

λ – выбранный порог.

Предложенный каскадный метод оказался устойчивым к набору преобразований,объединяющем преобразования и атаки, к которым были устойчивы голографический и нормализационный методы, то есть: вырезание фрагментов, форматирование JPEG, удаление строк и столбцов, добавление гауссовского шума, поворот, масштабирование.

В **заключении** даны основные результаты диссертационной работы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Произведено исследование устойчивости известного ранее «голографического» метода ЦВЗ к различным преобразованиям, найдены его уязвимости. Предложена модификация «голографического» метода с помощью введения «надежных» бит и весового декодирования. Устойчивость модифицированного метода на порядок превосходит устойчивость изначального метода для ряда атак и преобразований.

2. Предложен оптимальный метод извлечения ЦВЗ из фрагмента стеганограммы, который в полной мере учитывает параметры совершенной атаки вырезания. Как показали результаты моделирования, оптимальный метод извлечения дает достаточно малые вероятности ошибки извлечения бит и может быть успешно использован на практике.

3. Предложен каскадный способ вложения цифрового водяного знака, как объединение «голографического» и «нормализационного» методов вложения ЦВЗ с целью получения большей устойчивости к набору различных атак и

преобразований. Произведено моделирование каскадной системы ЦВЗ, позволившее экспериментально подтвердить стойкость водяного знака к таким видам преобразований, как добавление шума, вырезание фрагметов изображения, сжатие JPEG, вычеркивание строк и столбцов, изменение размеров изображения, поворот изображения.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

а) в рецензируемых научных изданиях

1. Кочкарёв, А.И. Голографические системы ЦВЗ с повышенной скоростью вложения / А.И. Кочкарёв // Телекоммуникации. – 2018. – № 8. – С. 30-37.

2. Кочкарёв, А.И. Решение проблемы извлечения информации для каскадной системы ЦВЗ при атаке вырезанием фрагментов изображения / А.И. Кочкарёв // Телекоммуникации. – 2016. – №. 10. – С. 27-38.

3. Кочкарёв, А.И. Система цифровых водяных знаков с повторным вложением информации по различным алгоритмам / В. И. Коржик, А. И. Кочкарев, Д. А. Флаксман // Телекоммуникации. – 2014. – №. 7. – С. 22-33.

б) в изданиях, индексируемых в международных базах цитирования:

4. Korzhik, V.I. Fingerprinting System for Still Images Based on the Use of a Holographic Transform Domain / V.I. Korzhik, G. Morales-Luna, A. Kochkarev, I. Shevchuk // In FedCSIS, M. Ganzha, L.A. Maciaszek, and M. Paprzycki, Eds., 2013, pp. 585–590.

5. Korzhik, V.I. Concatenated Digital Watermarking System Robust to Different Removal Attacks / V.I. Korzhik, G. Morales-Luna, A. Kochkarev, D. Flaksman // Computer Science and Information Systems. 2014. V. 11. No. 4. P. 1581-1594.

б) в других изданиях:

6. Кочкарев, А.И. Обнаружение нелегальных распространителей копий неподвижных изображений с помощью голографических методов вложения ЦВЗ / А.И. Кочкарёв // Труды учебных заведений связи. – 2011. – № 184. – С. 95-101.

7. Кочкарёв, А.И. Исследование системы цифровых водяных знаков устойчивой к их извлечению из фрагментов изображения / В.И. Коржик, А.И. Кочкарев // 63-я научно-техническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов: материалы / ГОУВПО СПбГУТ. – СПб., 2011. – С. 222-223.

8. Кочкарёв, А.И. Исследование «нормализации» изображений как средства обеспечения устойчивости ЦВЗ к случайным и преднамеренным преобразованиям / В.И. Коржик, А.И. Кочкарев, Д.А. Флаксман // Актуальные проблемы инфотелекоммуникаций в науке и образовании. Международная научно-техническая и научно-методическая конференция : сб. науч. ст. – 2013. – С. 821-824.

9. Кочкарев, А.И. Использование каскадирования систем ЦВЗ для обеспечения устойчивости к широкому спектру атак и преобразований / А.И. Кочкарев, Д.А. Флаксман // II

Международная научно-техническая и научно-методическая конференция : сб. науч. ст. – 2014. – С. 286-291.

10. Кочкарёв, А.И. Цифровая стеганография и цифровые водяные знаки. Часть 2 Цифровые водяные знаки / В.И. Коржик, С.О. Анфиногенов, А.И. Кочкарев, И.А. Федянин, А.Г. Жувикин, Д.А. Флаксман, В.Г. Алексеев. – СПбГУТ. – СПб., 2017.

Подписано в печать 09.10.2019. Формат 60×84 1/16.
Печ. л. 1,0. Тираж 100 экз.
Отпечатано в СПбГУТ, 193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1